UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/064,275	06/27/2002	Philip Lee Childs	RPS920020105	2694

53493	7590	07/17/2006

LENOVO (US) IP Law
Mail Stop ZHHA/B675/PO Box 12195
3039 Cornwallis Road
RTP, NC 27709-2195

EXAMINER
PATEL, NIRAV B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/064,275	CHILDS ET AL.
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>25 April 2006 (Amendment)</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-18</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-18</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on April 25, 2006 has been entered.   Claims 1, 2, 3,

10,11 and 12 are amended by the applicant. Claims 1-18 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 and 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Calvez et al (US Patent No. 6,981,145) and in view of Sadovsky (US Patent No.

5,689,638).

As per claim 1, Calvez teaches:

submitting a user authentication request to said authentication server [Fig. 1, 2]; in

response to a successful user authentication; receiving an authenticated user credential

which is unique to said user; storing said authenticated user credential on said client

utilizing a security method to prevent tampering with the credential [Fig. 1, col. 3 lines

56-66, col. 4 lines 12-28, col. 1 lines 13-14];

determining whether said authentication server is in operative communication with said client; in response to a determination that said authentication server is not in operative communication with said client [col. 1 lines 60-67, col. 3 lines 16-18, Fig. 1];

searching said client for a stored authenticated credential corresponding to said user; in response to finding an authenticated credential corresponding to said user, using said stored authenticated credential to access said at least on secure resource while said authentication server is not in operative communication with said client [col. 4 lines 60-67, col. 5 lines 7-20, col. 8 lines 4-11, 30-35, Fig. 1, col. 1 lines 60-63]; and in response to not finding an authenticated credential corresponding to said user, failing the user authentication request [col. 3 lines 62-63].

Calvez teaches the remote authentication using the user credential, transmits the authorization and a secret to the user [col. 3 lines 56-66] and the local machine stores the secret in the storage means [col. 4 lines 25-28]. Calvez doesn't expressively mention that using said authenticated credential to *access said at least one secure resource*.

However, Sadovsky teaches that using said authenticated credential to access said at least one secure resource [col. 8 lines 2-10].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Sandovsky with Calvez to utilize the authenticated credential, which is stored in the client machine, since one would have been motivated to access the protected resources [Sandovsky, col. 1 line 25, Calvez, col. 1 line 14].

As per claim 2, the rejection of claim 1 is incorporated and Calvez teaches:

in response to a determination that said authentication server is in operative communication with said client (the network component or server is available and the remote authentication is performed to authenticate the user i.e. normal mode): erasing from said client any stored authenticated credential corresponding to said user [col. 8 lines 12-14, col. 9 lines 4-7, col. 10 lines 17-18]; and failing said user authentication request [col. 3 lines 62-63].

3. Claims 3-8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calvez et al (US Patent No. 6,981,145) in view of Sadovsky (US Patent No. 5,689,638) and in view of Misra et al (US Paten No. 5,757,920).

As per claim 3, the rejection of claim 2 is incorporated and Calvez teaches that the authentication credential is stored on the client [Fig. 1, col. 4 lines 24-28]. Calvez doesn't expressively mention a set of security policies.

Misra teaches that implementing a set of security policies limiting the use of authenticated credentials stored on said client to access said at least one secure resource depending on a defined sensitivity of said at least one resource [Fig. 2B, col. 9 lines 34-36, col. 4 lines 15-17, col. 5 lines 58-65].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Misra with Calvez and Sandovsky, since one would have been motivated to access the protected resources [Calvez, col. 1 line 14].

As per claim 4, the rejection of claim 1 is incorporated and Misra teaches:

security method is encryption of the credential (i.e. logon credential) [col. 4 lines 17-19].

As per claim 5, the rejection of claim 1 is incorporated and Misra teaches:

security method is Public Key Infrastructure [col. 5 lines 22-26].

As per claim 6, the rejection of claim 1 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 7, the rejection of claim 2 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

As per claim 8, the rejection of claim 2 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 9, the rejection of claim 2 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

4. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calvez et al (US Patent No. 6,981,145) in view of Sadovsky (US Patent No. 5,689,638) and in view of Fuh et al (US Patent No. 6,463,474).

As per claim 10, Calvez teaches:

submitting a user authentication request to said authentication server [Fig. 1, 2]; in response to a successful user authentication; receiving an authenticated user credential which is unique to said user; storing said authenticated user credential on said client utilizing a security method to prevent tampering with the credential [Fig. 1, col. 3 lines 56-66, col. 4 lines 12-28, col. 1 lines 13-14];

determining whether said authentication server/gateway are in operative communication with said client; in response to a determination that said authentication server/gateway are not in operative communication with said client (i.e. network connection or other components are down or unavailable) [col. 1 lines 60-67, col. 3 lines 16-18, Fig. 1];

searching said client for a stored authenticated credential corresponding to said user; in response to finding an authenticated credential corresponding to said user, using said stored authenticated credential to access said at least on secure resource while said gateway is not in operative communication with said client [col. 4 lines 60-67, col. 5 lines 7-20, col. 8 lines 4-11, 30-35, Fig. 1, col. 1 lines 60-63]; and in response to not finding an authenticated credential corresponding to said user, failing the user authentication request [col. 3 lines 62-63].

Calvez teaches the remote authentication using the user credential, transmits the authorization and a secret to the user [col. 3 lines 56-66] and the local machine stores the secret in the storage means [col. 4 lines 25-28]. Calvez doesn't expressively mention that using said authenticated credential to *access said at least one secure resource.*

However, Sadovsky teaches that using said authenticated credential to access said at least one secure resource [col. 8 lines 2-10].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Sandovsky with Calvez to utilize the authenticated credential, which is stored in the client machine, since one would have been motivated to access the protected resources [Sandovsky, col. 1 line 25, Calvez, col. 1 line 14].

Calvez and Sadovsky don't expressively mention that storing the authenticated credential on said gateway utilizing a security method to prevent tampering with the credential.

However, Fuh teaches that storing the authenticated credential on said gateway utilizing a security method to prevent tampering with the credential [Fig. 4, col. 12 lines 45-47, col. 9 lines 57-63].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Fuh with Calvez and Sandovsky to store the authentication information on the gateway (or firewall, router), since one would have been motivated to access the protected resources [Sandovsky, col. 1 line 25, Calvez, col. 1 line 14].

As per claim 11, the rejection of claim 10 is incorporated and Fuh teaches:

in response to a determination that said gateway is in operative communication with said client; searching the gateway for an authenticated credential corresponding to said user [Fig. 3, 4, 7A col. 10 lines 36-45]; in response to finding an authenticated credential corresponding to said user, using said authenticated credential to access said at least one secure resource [Fig. 4, 7A col. 15 lines 31-35, col. 13 lines 1-6, Fig. 5B]; in response to not finding an authenticated credential corresponding to said user, failing the user authentication request [Fig. 7A col. 10 lines 51-58, col. 11 lines 29-33];

erasing from the gateway any authenticated credential corresponding to said user [col. 14 lines 43-47].

Calvez teaches:

in response to a determination that said authentication server is in operative communication with said client (the network component or server is available and the remote authentication is performed to authenticate the user i.e. normal mode) [Fig. 1]:

erasing from the client any authenticated credential corresponding to said user [col. 8 lines 12-14, col. 9 lines 4-7, col. 10 lines 17-18]; and failing said user authentication request [col. 3 lines 62-63].

5. Claims 12-17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calvez et al (US Patent No. 6,981,145) in view of Sadovsky (US Patent No. 5,689,638) in view of Fuh et al (US Patent No. 6,463,474) and in view of Misra et al (US Paten No. 5,757,920).

As per claim 12, the rejection of claim 11 is incorporated and Calvez teaches that authentication credential stored on the client [Fig. 1, col. 4 lines 24-28]. Calvez doesn't expressively mention a set of security policies.

Misra teaches that implementing a set of security policies limiting the use of authenticated credentials stored *on said client* or said gateway to access said at least one secure resource depending on a defined sensitivity of said at least one resource [Fig. 2B, col. 9 lines 34-36, col. 4 lines 15-17, col. 5 lines 58-65].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Misra with Calvez, Sandovsky and Fuh, since one would have been motivated to access the protected resources [Calvez, col. 1 line 14].

As per claim 13, the rejection of claim 10 is incorporated and Misra teaches:

security method is encryption of the credential (i.e. logon credential) [col. 4 lines 17-19].

As per claim 14, the rejection of claim 10 is incorporated and Misra teaches:

security method is Public Key Infrastructure [col. 5 lines 22-26].

As per claim 15, the rejection of claim 10 is incorporated and it encompasses limitations that are similar to limitations of claim 14. Thus, it is rejected with the same rationale applied against claim 14 above.

As per claim 16, the rejection of claim 11 is incorporated and it encompasses limitations that are similar to limitations of claim 13. Thus, it is rejected with the same rationale applied against claim 13 above.

As per claim 17, the rejection of claim 11 is incorporated and it encompasses limitations that are similar to limitations of claim 14. Thus, it is rejected with the same rationale applied against claim 14 above.

As per claim 18, the rejection of claim 11 is incorporated and it encompasses limitations that are similar to limitations of claim 15. Thus, it is rejected with the same rationale applied against claim 15 above.

Response to Amendment

6. Applicant has amended claims 1, 2, 3, 10, 11 and 12 which necessitated new ground of rejection. See rejection above.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.   Accordingly, **THIS ACTION IS MADE FINAL**.   See MPEP § 706.07(a).   Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP

6/28/06
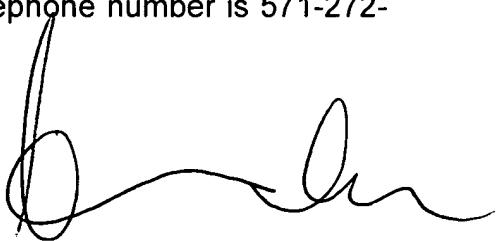
KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100